

SESSION

COPILOT AGENT MANAGEMENT

So bekommst du deine Agents in den Griff
entlang des gesamten Lifecycles

Microsoft 365 Copilot | Agent Governance

 14.10.2026

 14.00 Uhr

 Rheingoldhalle, Mainz

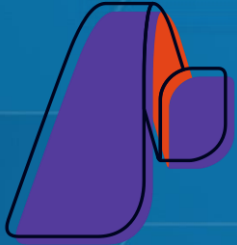


Daniel Rohregger
glueckkanja AG



Welche **Agents** haben wir eigentlich? Wem gehören sie? Und dürfen sie, was sie tun?

— Die drei Fragen, die in fast jedem Tenant offen sind.



AGENTS.

DEIN AGENT IST SCHNELL EINE EIGENE SOFTWARE

Agents sind Custom Apps.

Schneller gebaut, von mehr Menschen gebaut, aber mit denselben Pflichten wie jede andere Anwendung im Unternehmen.



Verantwortung

Ein Owner, der zuständig bleibt



Anforderungen

Zweck, Zielgruppe, Daten, Kosten



Tests

Qualität und Sicherheit vor dem Go-live



Freigabe

Ein Gate, das zum Risiko passt



Betrieb

Inventar, Nutzung, Kosten



Stilllegung

Geplantes Ende statt Wildwuchs



Daniel Rohregger
glueckkanja AG

Hi, ich bin Daniel

- Cloud Architect M365 & AI, glueckkanja AG
- Copilot Trainer & Coach, Copilot Coaching
- Podcast: 365 Checkpoint
- daniel.rohregger@glueckkanja.com · daniel@copilot-coaching.de



AGENDA FÜR UNSERE HEUTIGE SESSION

- 1 **Warum Agents eigene Software sind**
- 2 **Agent-Readiness als Basis**
- 3 **Der Agent Governance Lifecycle**
- 4 **Aus der Praxis: Umsetzung bei einem Kunden**
- 5 **Live-Demos**
- 6 **Takeaways**

01

ABSCHNITT

EINORDNUNG

Wir gehen davon aus: Dein Tenant ist agent-ready

ZEHN SCHRITTE ZUM AGENT-READY TENANT



Agent Readiness in M365: Der 10-Schritte-Blueprint (2026) | Daniel Rohregger (MVP)

1

Kern-Tenant-Einstellungen prüfen

2

Agent 365 aktivieren und verstehen

3

Oversharing

Public Teams prüfen

4

Oversharing

SharePoint-Baseline-Report erstellen

5

Oversharing

Site-Owner in Access Reviews einbinden

6

Oversharing

Prozess gegen Oversharing etablieren

7

Oversharing

Sensitivity Labels und DLP anwenden

8

Power Platform Governance umsetzen

9

Copilot-Credit-Modell festlegen

10

Heute

Agent- & AI-Asset-Lifecycle definieren

JEDER KANN JETZT AGENTS BAUEN



SharePoint Agents

Erstellt direkt auf der Site, von allen mit Bearbeitungsrechten.

Gespeichert als .agent-Datei, geteilt über Teams.



Agent Builder

Im Microsoft Copilot App, für sich selbst oder kleine Teams.

Ohne Code: Anweisungen plus Wissensquellen.



Copilot Studio

Für Maker und Entwickler in Power-Platform-Umgebungen.

Mit Aktionen, Flows und Connectoren.



Microsoft Foundry

Pro-Code-Agents in Azure.

Automatisch in der M365 Agent Registry veröffentlicht.

Persönliche Agents: arbeiten im Auftrag einzelner Nutzer



Copilot Cowork

Agentischer Modus in M365 Copilot – führt delegierte Aufgaben über mehrere Apps aus.

Lange Laufzeiten, komplexe Aufgaben, handelt im Namen des Benutzers.



Autopilot(s)

Always-on Autopilot (Preview, Frontier-Programm) – basiert auf GitHub Copilot.

Arbeitet proaktiv im Hintergrund – lokal und in der Cloud, mit Dateien und Browser.

02

ABSCHNITT

DER AGENT (GOVERNANCE) LIFECYCLE

Agents entstehen, laufen, altern und manche sterben

DER AGENT GOVERNANCE LIFECYCLE AUF EINEN BLICK

Über alle Phasen: Einstufung (Tier) · Ownership · Kosten · Richtlinien



Governance Board: prüft den Prozess quartalsweise und schärft Regeln, Fristen und Schwellen nach.

03

ABSCHNITT

PHASE 1: ENTSTEHEN

Wer darf wo welche Agents bauen?

1 Entstehen

2 Bauen und Testen

3 Freigeben

4 Betreiben

5 Prüfen

6 Stilllegen

SIEBEN FRAGEN VOR DEM BAU

01

Problem

Welches Problem lösen wir, und für wen?

02

Workflow

Welche Schritte, Entscheidungen und Übergaben gibt es?

03

Trigger

Was startet den Prozess: Person, Ereignis oder Zeitplan?

04

Daten

Welche Datenquellen braucht es, und wer darf zugreifen?

05

Erster Nutzen

Was ist der kleinste Schritt, der sofort hilft?

06

Ownership

Wer liefert fachlichen Kontext, wer technische Expertise?

07

Betrieb

Einmal eingerichtet oder dauerhaft betrieben?

Plus Governance

Tier, intern oder extern, Budget

FÜNF WEGE DER ENTSTEHUNG, FÜNF ANTWORTEN

Plattform	Wer baut	Steuerung beim Entstehen	Governance-Schwerpunkt
 Agent Builder und SharePoint Agents	Alle Mitarbeitenden	Kaum begrenzen: eingebaut und gewollt	Teilen, Wissensquellen, Oversharing
 Copilot Studio	Maker, Fachbereiche, IT	Persönl. Produktivität freigeben, Dev- und feste Environments per Antrag	Power Platform Governance: Managed Environments, Connector-DLP
 Microsoft Foundry	Pro-Code-Teams	Immer projektbasiert: Ressourcen und Projekte nur per Antrag	Azure-Governance, Identitäten, Kosten
 Pers. Agents (Copilot Cowork, Microsoft Scout)	Microsoft, aktiviert pro Nutzer	Verfügbarkeitsfrage: Wer bekommt Zugriff?	Plugins und MCP-Server erlauben oder sperren, Kosten
 Partner-Agents 3rd Party Agents	Externe Anbieter Dots, Grok, Claude	Freigabe je Publisher-Typ	Datenabfluss, Vertrag

Agent Governance heißt: jede Plattform im Griff und plattformübergreifend handeln.

COPILOT STUDIO: BEST PRACTICES

1

Default Environment

Persönliche Produktivität anbieten? Token-Limits & Default absichern.

2

Developer Environments

Eigene Sandbox pro Maker, gesteuert über Environment Routing.

3

Managed Environments

Je Abteilung oder Use Case für produktive Agents, mit Sharing-Limits.

4

Connector-DLP

Erlaubte Connectoren, Wissensquellen und MCP-Server definieren.

5

Beantragungsprozess

Feste Environments nur mit Owner, Zweck, Tier und Budget.

Security

Overview

Settings

Data and privacy

Identity and access

Threat detection

Compliance

Products

Power Pages



Threat detection

Protect your organization and its assets with tools that help you discover anomalies, then take quick action to imp

Additional threat detection and protection for Copilot Studio agents PREVIEW

Runtime Protection - Add an extra layer of real-time threat defense to protect your agents. Integrate moni
threats like prompt injection attacks during agent runtime.

Microsoft Defender - Copilot Studio Agents PREVIEW

Microsoft Defender - based threat detection capabilities for Copilot Studio Agents

Showing images and URLs PREVIEW

Control whether agent responses can display images and URLs. Images and links can be a security risk bec
information.

Sharing agents with embedded maker credentials PREVIEW

Control whether makers can share agents that include their own credentials.

AGENT: TIERING MODELL

Tipp: Nutzt euer bestehendes Klassifizierungsschema, statt ein neues zu erfinden.

Das ist ein Beispiel:

Plus Template: persönliche Agents als Vorlage zum Kopieren, ohne eigenen Lifecycle.

Persönlich

Ein Nutzer, eigene Produktivität.
Kommt nie in den Katalog.

kein Review

Team

Produktivität im Team.
Team-owned.
Katalogkandidat, wenn geteilt.

Review jährlich, optional

Business Important

Grauzone: Fachbereich und IT.

Explizite Ownership, Business Sponsor.

Review halbjährlich

Business Critical

Automatisiert oder ersetzt einen Geschäftsprozess.

IT-owned, Security Review Pflicht.

Review quartalsweise

04

ABSCHNITT

PHASE 2: BAUEN UND TESTEN

Welche Standards gelten, bevor ein Agent live geht?

1 Entstehen

2 Bauen und Testen

3 Freigeben

4 Betreiben

5 Prüfen

6 Stilllegen

TESTSTANDARDS JE TIER

Persönlich und Team

- Selbsttest mit Checkliste
- Nur eigene oder Team-Daten
- Keine Freigabe nötig

Business Important

- Testfälle für die Kernfragen
- Peer-Review von Anweisungen und Wissen
- Datenzugriff geprüft

Business Critical

- Evaluation mit Testsets
- Stresstest unter Last
- Versuchen, den Agent zu brechen
- Security Review

Extern wirksam

- Alles aus Business Critical
- Prompt-Injection- und Missbrauchstests
- Rechts- und Datenschutzprüfung
- Optional externe Prüfung

LEAST PRIVILEGE



Daten minimieren

Nur benötigte Wissensquellen aus dem überschüssigen Altbestand.



Tools minimieren

MCP-Server bereitstellen und aktivieren.



Eigene Identität

Entra Agent ID statt Erste Agents.

Travel Process Agent

Published

Erstellen

Vorschau

Auswerten

Überprüfen



Überprüfen

Veröffentlichen



Travel Process Agent



Anweisungen



Your goal is to do an interview with me about my last travel and therefore generate a list of

1. Travel Location
2. Duration
3. Hotel Name (based on the invoice)
4. Traveltype (Car, Plane, Train)

After that, use the OneDrive MCP to search for my invoices that are in a folder.

Modell

Claude Fable 5.1



Qualifikationen

Verhaltensweisen durch strukturierte Anweisungen festlegen



Werkzeuge

Agent mit externen Systemen und Aktionen verbinden



Wissen

Vertrauenswürdigen Kontext zur Entscheidungsfindung bereitstellen



Verbundene Agents

Zusammenarbeiten zwischen Agents, um die Arbeit abzuschließen



Speicher Vorschau

Dem Agenten erlauben, sich Informationen zu merken und sie zur Verbesserung zukünftiger Antworten zu verwenden.

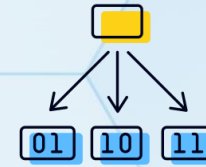


AGENTS SIND SOFTWARE: GUIDANCE, SCHULUNG, SUPPORT



Richtlinie für Ersteller

Was ist erlaubt, welche Daten, welche Tools, welche Grenzen.



Vorlagen

Geprüfte Templates als Startpunkt statt jedes Mal bei null.



Schulung

Rollenbasierte Lernpfade für Maker, Owner und Champions.



Review-Checklisten

Je Tier, damit Prüfungen vergleichbar und schnell sind.



Hackathons

Gemeinsam bauen und Use Cases schärfen, bevor es teuer wird.



Sprechstunde

Ansprechpartner für Fragen vor dem Bau, nicht erst danach.

05

ABSCHNITT

PHASE 3: FREIGEBEN

Wer sagt Ja und auf welcher Grundlage?

1 Entstehen

2 Bauen und Testen

3 Freigeben

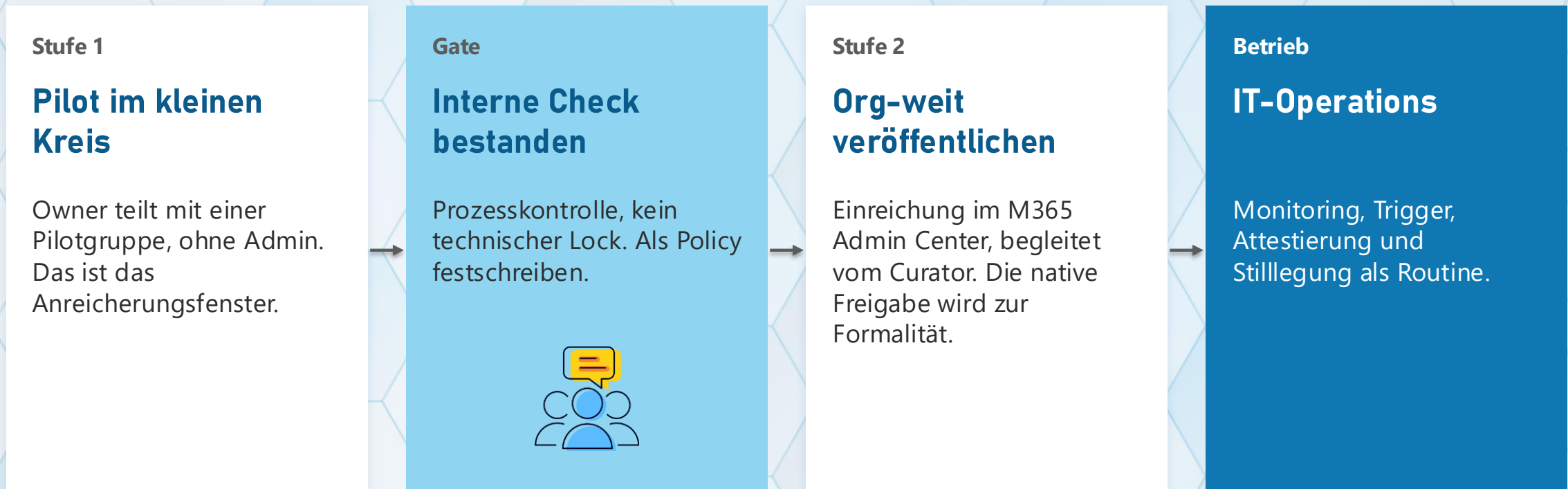
4 Betreiben

5 Prüfen

6 Stilllegen

VOM POC IN DEN BETRIEB: SEQUENZIEREN STATT INTEGRIEREN

Zwei Freigabe-Gates parallel machen eines zur Dekoration. Die native Freigabe kennt weder Business Case noch Risiko.



Voraussetzung: Wer im Admin Center Publish-Anfragen freigibt, ist an den Governance-Prozess gekoppelt.

06

ABSCHNITT

PHASE 4: BETREIBEN

Was du nicht kennst, kannst du nicht steuern

1 Entstehen

2 Bauen und Testen

3 Freigeben

4 Betreiben

5 Prüfen

6 Stilllegen

NUR INVENTAR IST NICHT GOVERNANCE



Agent 365

Was die Plattform liefert

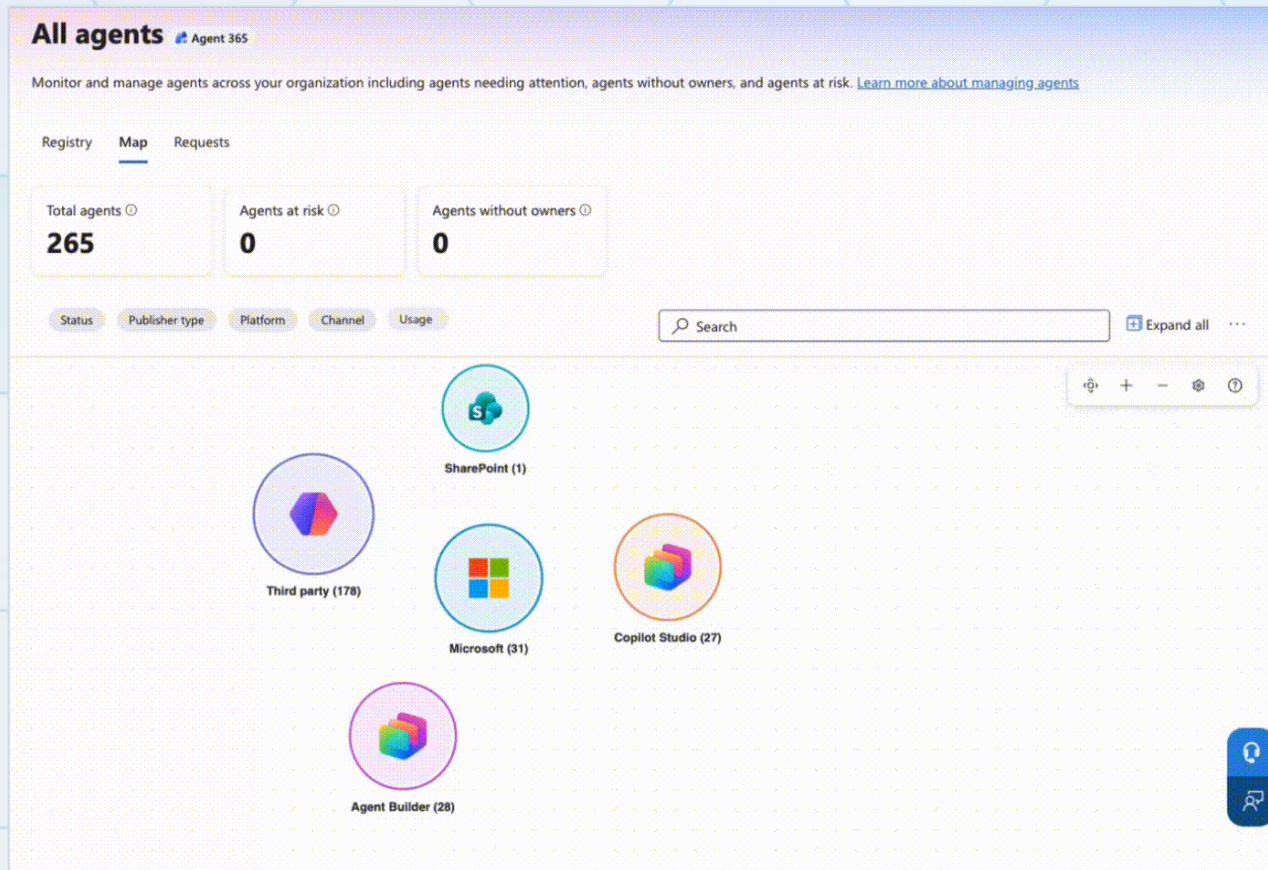
- Name, Plattform, Publisher
- Status und Version
- Kanäle (Teams, Outlook, Copilot)
- Technischer Owner, falls gesetzt
- Anweisungen (System Prompt)
- Aktive Nutzer und Sessions
- Freigaben an Nutzer und Gruppen
- Zugriff auf SharePoint und OneDrive

Was ein Mensch bestätigen muss

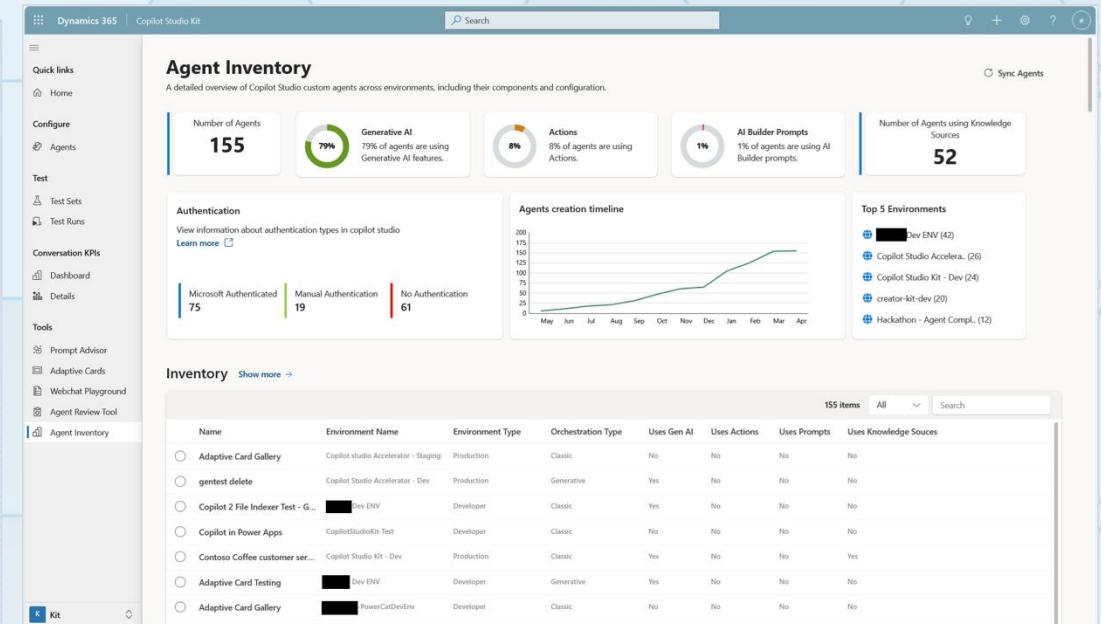
- Verantwortlicher Owner
- Business Sponsor
- Zweck und Business Case
- Tier und Kritikalität
- Datensensitivität
- Autonome Aktionen
- Auswirkung bei Ausfall
- Erwartete Nutzerzahl
- Nächstes Review
- Freigabe zur Veröffentlichung

Die Registry zeigt, was existiert. Ob ein Agent existieren sollte und wer dafür verantwortlich ist, weiß nur ein Mensch.

INVENTAR IN AGENT 365 UND POWER PLATFORM



Agent 365: Map



Copilot Studio Kit: Agent Inventory

All agents Agent 365

Monitor and manage agents across your organization including agents needing attention, agents witho

Registry Requests Local agents **Frontier**

Total agents ⓘ **423** Agents at risk ⓘ — Agents without owners ⓘ **0**

WER IST EIGENTLICH VERANTWORTLICH?

Technischer Ersteller

≠

verantwortlicher Owner

Das Owner-Feld ist oft leer oder nennt nur, wer den Agent angelegt hat.

Accountability muss ein Mensch bestätigen und pflegen.

Entra Agent ID macht Sponsors zur Pflicht. Verknüpft sie mit eurem Rollenmodell.

Technischer Ersteller

Hat den Agent gebaut. Nicht automatisch verantwortlich.

Confirmed Owner

Übernimmt die Verantwortung im Alltag. Von einem Menschen bestätigt.

Business Sponsor

Ab Business Important. Trägt Budget und Lizenz, nicht nur die Unterschrift.

Data/Platform Responsible

Verantwortet die Daten, wenn sie einer anderen Plattform gehören.

Curator

Betreibt Intake, pflegt den Katalog, setzt Governance-Aktionen um.

Security und Compliance

Prüft Business Critical und alles mit personenbezogenen Daten.

Agent-Approval Group

Tagt regelmäßig, entscheidet über Einstufungen, kann sofort sperren.

Prinzip

Jede Rolle ist eine Person oder ein Gremium mit Namen, kein Postfach.

Erkenntnis 03 · Ownership bestätigt ein Mensch. Technische Ersteller sind ein Hinweis, keine

07

ABSCHNITT

PHASE 5 UND 6: PRÜFEN UND STILLLEGEN

Kein Lebenszeichen, kein Betrieb

1 Entstehen

2 Bauen und Testen

3 Freigeben

4 Betreiben

5 Prüfen

6 Stilllegen

LEBENSZEICHEN STATT HOFFNUNG

Situation	Reaktion	Womit
Owner reagiert nicht	Erinnerung, letzte Warnung, Sperre	Eskalations-Flow, Sperre über Agent 365
Agent wird nicht mehr genutzt	Review oder Sperre	Agent-365-Regel für ungenutzte Agents ohne Owner, Nutzungsdaten
Business Critical nicht rezertifiziert	Automatische Sperre	Attestierung je Tier
Owner verlässt das Unternehmen	Neuzuweisung an die Führungskraft	Agent-365-Regel, Entra Sponsor-Workflow
Nutzung übersteigt Deklaration	Review-Aufgabe mit Begründung	Trigger-Flow

08

ABSCHNITT

AUS DER PRAXIS

So haben wir es bei einem Kunden umgesetzt, beispielhaft

LÖSUNGEN ENTLANG DES LIFECYCLES



Beispielhaft: eine Umsetzung von vielen möglichen, gebaut auf Microsoft 365 und Power Platform.

DIE AGENT GOVERNANCE SOLUTION IM ÜBERBLICK



Agent DB

Ein Datensatz pro Agent, egal aus welcher Quelle. Dataverse als System of Record.



Anreicherung

Owner liefern Governance-Daten per Adaptive Card direkt in Teams.



Eskalation und Sperre

Erinnerung, letzte Warnung, Manager, Sperre über Agent 365.



Agent-Galerie

Self-Service-Katalog für alle Mitarbeitenden, in SharePoint und Teams.



Katalog-Agent

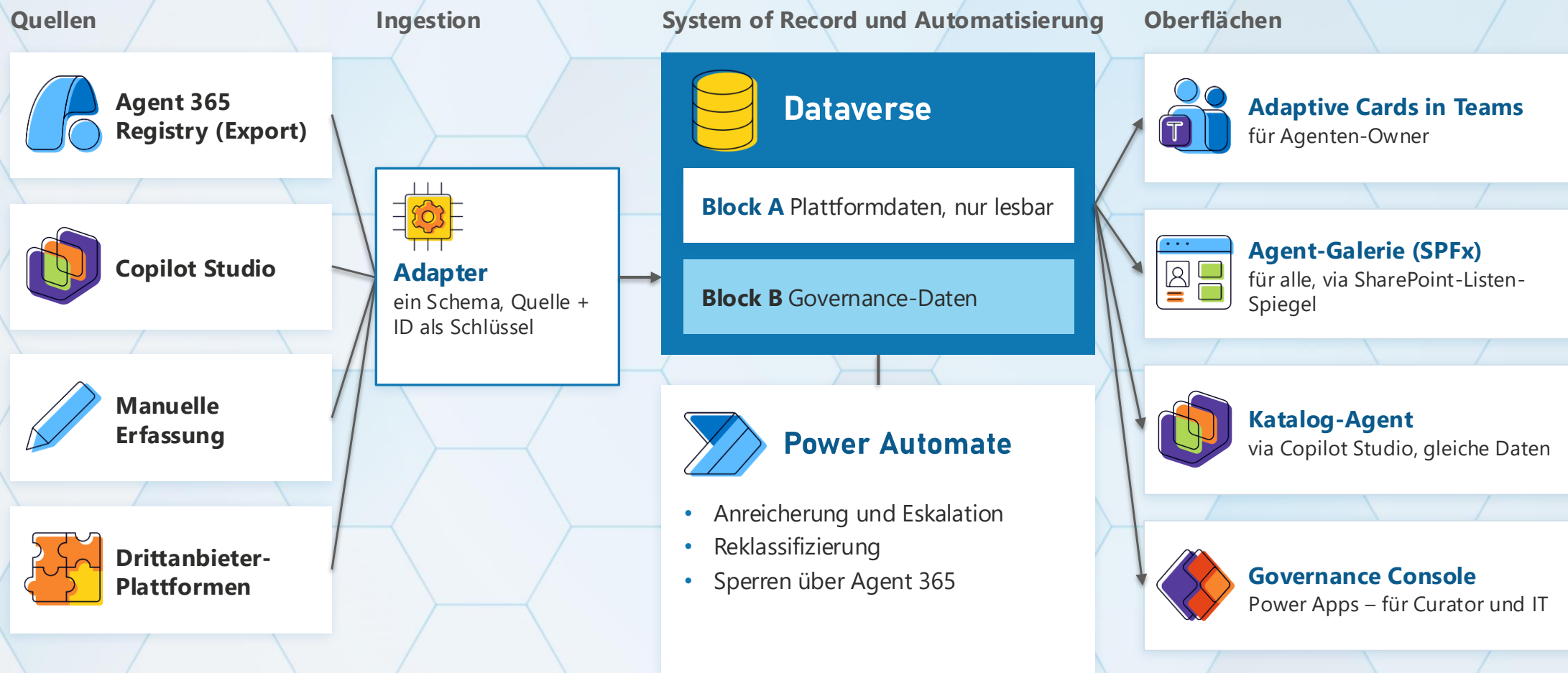
Empfehlungen in natürlicher Sprache, auf denselben Daten.



Governance Console

KPIs, Action Items und Aktionen für Curator und IT.

ARCHITEKTUR DER AGENT GOVERNANCE SOLUTION



Erkenntnis 06 · Lizenzen gehören in die Architektur. Lesezugriff kann sechsstellig kosten.

Agent Governance Enrichment

Complete the governance information below. Submissions support ownership validation, risk classification, review routing, and Agent Store readiness.

Agent Overview

Agent Name: AgentWhistler_classic
Detected Channels:

Ownership

Define who is accountable for this agent and its underlying data.

Confirmed Owner *

Accountable owner for governance follow-ups.

Business Sponsor

Leave blank if same as Confirmed Owner.

Data Responsible

Responsible person for the underlying data or platform context. Leave blank if same as Confirmed Owner.

Agent Classification

Categorize the agent and describe its intended audience.

Category *

Data Sensitivity *

Short Description *

Audience Tags *

Risk and Impact

These signals drive governance routing and review depth.

Business Impact *

Expected Agent Users *

ANREICHERUNG IN TEAMS



Ownership

Confirmed Owner, Business Sponsor, Data Responsible

Klassifizierung

Kategorie, Datensensitivität, Kurzbeschreibung, Zielgruppen

Risiko und Wirkung

Business Impact, erwartete Nutzer, autonome Aktion, Galerie

- Eine Adaptive Card im Chat, keine App, kein Portal
- Felder passen sich dem Tier an
- Antworten landen direkt im Governance-Datensatz
- Pflichtfelder statt Freitext, wo es geht

ANREICHERUNG IN TEAMS



Ownership

Confirmed Owner, Business Sponsor, Data Responsible

Klassifizierung

Kategorie, Datensensitivität, Kurzbeschreibung, Zielgruppen

Risiko und Wirkung

Business Impact, erwartete Nutzer, autonome Aktion, Galerie

- Eine Adaptive Card im Chat, keine App, kein Portal
- Felder passen sich dem Tier an
- Antworten landen direkt im Governance-Datensatz
- Pflichtfelder statt Freitext, wo es geht

Ownership

Define who is accountable for this agent and its underlying data.

Confirmed Owner *

Accountable owner for governance follow-ups.

Business Sponsor

Leave blank if same as Confirmed Owner.

Data Responsible

Responsible person for the underlying data or platform context. Leave blank if same as Confirmed Owner.

Agent Classification

Categorize the agent and describe its intended audience.

Category *

Data Sensitivity *

Short Description *

Audience Tags *

Risk and Impact

These signals drive governance routing and review depth.

Business Impact *

Expected Agent Users *

☐ Autonomous Action

Does the agent act autonomously without user interaction?

☐ Publish to Gallery

Make this agent available to everyone in the Agent Gallery?

Before submitting

Verify ownership, data sensitivity, autonomous-action capability, business impact, and expected user count. These fields influence governance routing.

[Submit Governance Details](#)

ESKALATION AUTOMATISCH – GESTEUERT ÜBER REMINDER & ZEIT



Konfiguration, nicht Policy

Alle Fristen sind Umgebungsvariablen.
Jeder Kunde stellt sie selbst ein.

Frist bleibt Frist

Erneutes Senden einer Karte verlängert die Sperrfrist nie.

Karten ohne Zustand

Vor jedem Schreiben wird der Datensatz geprüft. Doppelte Karten sind harmlos.

ERINNERUNG, WARNUNG, ESKALATION & SPERRE

Workflows 4:04 PM


Agent Details Required

First reminder

We have not yet received the required governance information for this agent.

Agent overview

Agent	AgentWhistler_classic
Agent ID	a06693e9-937f-f111-ab0f-7ced8d44e4b1
Owner	adm.dr@c4a8v.org
Status	Agent details requested
Details initially Requested on	07/16/2026 14:29:00

Why this information is required

Complete agent information provides a reliable overview of our agents and AI infrastructure. It supports clear ownership, lifecycle management, risk assessment, governance reviews, and effective support.

Action required

The Adaptive Card for submitting the required agent details was sent directly above this reminder. Please complete and submit it as soon as possible.. If it is not visible yet, wait briefly and refresh the conversation.

If the information remains missing, a final warning will follow before further governance actions are taken.

Get support

Tag 14 Erinnerung

Workflows 4:24 PM


Final Warning: Agent Details Overdue

The required governance information has not been submitted within the expected timeframe.

Agent overview

Agent	AgentWhistler_classic
Agent ID	a06693e9-937f-f111-ab0f-7ced8d44e4b1
Owner	adm.dr@c4a8v.org
Status	Agent details overdue
Originally requested	2026-07-02T14:29:00Z

Manager notified

Your manager has been informed that we have not received the required agent details within the expected timeframe.

Immediate action required

The Adaptive Card for submitting the required agent details was sent directly above this warning. Complete and submit it immediately.

If the information remains missing, the agent will be blocked for you and all other users until the governance requirements have been completed and reviewed.

Get support

Tag 28 Letzte Warnung

Agent Governance Escalation

Required governance information for an agent owned by one of your team members remains outstanding.

Escalation details

Agent	AgentWhistler_classic
Owner	adm.dr@c4a8v.org
Owner email	adm.dr@c4a8v.org
Originally requested	07/02/2026 14:29:00
Current status	Final warning issued

Reason for this notification

The agent owner has not submitted the required governance information within the expected timeframe, despite receiving the initial request and a reminder.

The owner has now received a final warning. If the information remains missing, the agent will be blocked for the owner and all other users until the governance requirements have been completed and reviewed.

Optional Führungskraft

Workflows 8:10 PM


Agent Blocked

Tag 35 Sperre

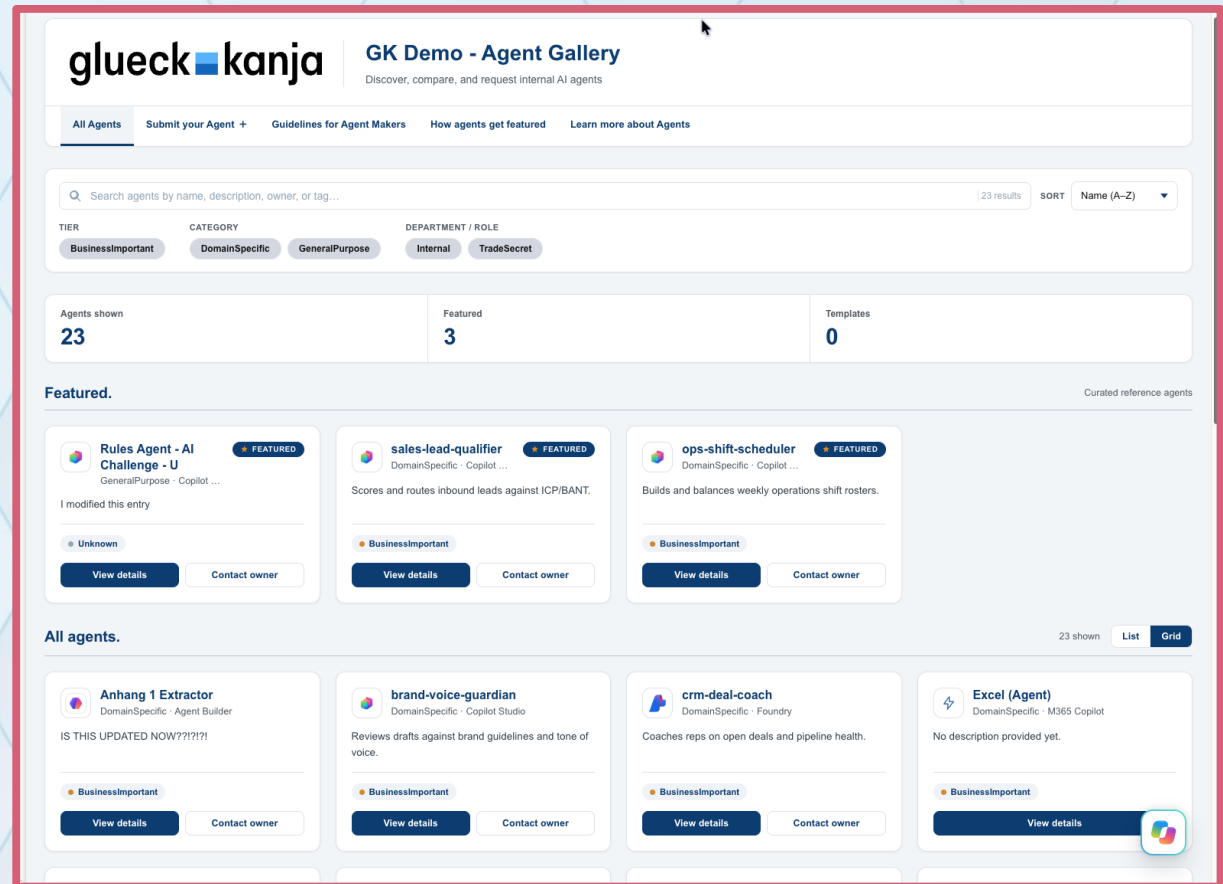
The agent **AgentWhistler_classic** has been blocked because the required governance information was not provided.

To learn more about the reactivation process, use the button below.

Reactivation information

LIVE DEMO 1: AGENT GALLERY

- Detailansicht mit Business Case, Owner, Tier und Datensensitivität
- Aktionen direkt auf der Karte: Zugriff anfragen, Problem melden
- Liest aus dem schreibgeschützten SharePoint-Listen-Spiegel
- Als SharePoint-Seite und als Teams-Tab



The screenshot displays the 'glueck kanja' Agent Gallery interface. The header includes the logo and the title 'GK Demo - Agent Gallery' with the subtitle 'Discover, compare, and request internal AI agents'. Navigation links include 'All Agents', 'Submit your Agent +', 'Guidelines for Agent Makers', 'How agents get featured', and 'Learn more about Agents'.

A search bar allows filtering agents by name, description, owner, or tag. Below the search bar, filters for 'TIER' (BusinessImportant, DomainSpecific, GeneralPurpose), 'CATEGORY', and 'DEPARTMENT / ROLE' (Internal, TradeSecret) are visible. Summary statistics show 23 agents shown, 3 featured, and 0 templates.

The 'Featured' section highlights three agents: 'Rules Agent - AI Challenge - U' (GeneralPurpose - Copilot), 'sales-lead-qualifier' (DomainSpecific - Copilot), and 'ops-shift-scheduler' (DomainSpecific - Copilot). Each agent card includes a description, a 'BusinessImportant' tag, and buttons for 'View details' and 'Contact owner'.

The 'All agents' section shows a grid of agents including 'Anhang 1 Extractor' (DomainSpecific - Agent Builder), 'brand-voice-guardian' (DomainSpecific - Copilot Studio), 'crm-deal-coach' (DomainSpecific - Foundry), and 'Excel (Agent)' (DomainSpecific - M365 Copilot). Each card also features a 'BusinessImportant' tag and action buttons.

LIVE DEMO 2: AGAD – AGENT GOVERNANCE ADMINISTRATIVE DASHBOARD

KPI-Karten

Nur Governance-Signale, keine Nutzungsanalyse.

Tier und Funnel

Verteilung und Fortschritt der Anreicherung auf einen Blick.

Action Items

Nach Schweregrad sortiert, jede Zeile klickbar.

Suche

Volltext, Fragmente, Tiers, Namen, IDs u. a.

Settings

Globale Parameter: BlockDays, URLs, Titel, Mail-Adressen u. a.

Vulcan SE

Agent Governance Admin Dashboard

Overview

Agents

Action items (1 high)

Activity

Operations

Settings

Agents

Search name, publisher, owner, description, agent ID

Refresh

View

Tier

Enrichment status

Enrichment

Published

All agents

All tiers

Awaiting review

All

All

Featured

All

No confirmed owner

Clear all

Awaiting

X

Name	Tier	Enrichment	Confirmed owner	Active users	Last used	Last ingested	Details
Agent365ParseCSVXLSX	Unclassified	Submitted	adm.dr@c4a8v.org	1 –	2026-08-24		Details
Anhang 1 Extractor	Personal template	Submitted	adm.dr@c4a8v.org	0 –	2026-08-24		Details
brand-voice-guardian	Team	Submitted	marco.reuter@c4a8v.org	0 –	–		Details
crm-deal-coach	Business important	Submitted	samuel.ortega@c4a8v.o...	0 –	–		Details
hr-onboarding-buddy	Team	Submitted	hannah.klein@c4a8v.org	0 –	–		Details
hr-policy-advisor	Business important	Submitted	hannah.klein@c4a8v.org	0 –	–		Details
hr-recruiting-screener	Business important	Submitted	hannah.klein@c4a8v.org	0 –	–		Details
it-helpdesk-triage	Business important	Submitted	ivan.petrov@c4a8v.org	0 –	–		Details
marketing-campaign-planner	Team	Submitted	marco.reuter@c4a8v.org	0 –	–		Details

STAND DER UMSETZUNG: RUND 80 PROZENT

Gebaut, getestet, läuft

- Katalog mit Sync aus dem Agent-365-Export
- Enrichment per Adaptive Card
- Eskalation bis zur Sperre
- Agent-Galerie und Katalog-Agent
- Governance Console mit Action Items
- Live-Sperren über die Agent-365-API

Kommt als Nächstes

- Full Code Review
- Kosten als feste Dimension im Lifecycle
- Inventar für Plugins, APIs und MCP-Server
- Self-Service für Owner

GEBAUT. GETESTET. BALD PRODUKTIV.

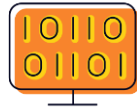
Die Agent Governance Solution ist **fertig entwickelt** und geht in Kürze beim ersten Kunden in Produktion. Ausgelegt als **Template für große Tenants.**

NICHT NUR AGENTS: PLUGINS, APIS UND MCP-SERVER



Plugins und Connectoren

Erweitern Copilot, Cowork und Agents um Fähigkeiten und Datenzugriffe.



APIs

Eigene Schnittstellen, die Agents aufrufen dürfen.



MCP-Server

Eigene und fremde Server mit Zugriff auf eure Systeme.

Inventar

Ownership

Freigabe

Lifecycle

Erster Hebel heute: Agent 365 steuert, welche Tools und MCP-Server Agents nutzen dürfen. Mittelfristig gehört alles in denselben Prozess.

DAS KANNST DU NÄCHSTE WOCHE IN DEINEM TENANT TUN

1

Inventar ziehen

M365 Admin Center > Agents > All agents > Export

2

Verwaiste Agents finden

Karte „Agents without owners“, Regel zur Neuzuweisung an Manager

3

Zugriff steuern

Agents > Settings: User access, Sharing, Agent and plugin access

4

Oversharing sichtbar machen

Data access governance reports im SharePoint Admin Center

5

Kosten deckeln

Abrechnungsrichtlinie: Budget, Alerts, Monatslimit/Agent

6

Tier-Modell festlegen

Bestehende Klassifizierung wiederverwenden

7

Curator benennen

Name, Vertretung und Kapazität pro Woche

8

Betriebsrat und DSB informieren

Bevor die erste Eskalation läuft

M M I T M A I N Z 2 0 2 6

N DANK!

n? Lass uns reden.

LinkedIn



Feedback

GIB UNS FEEDBACK!

- 1 QR-Code mit dem Handy scannen
- 2 Session Titel eingeben
- 3 Kurzes Feedback schriftlich hinterlassen

Dein Feedback: Die Sessions der
M365 Summit 2026



DANKE AN UNSERE SPONSOREN!

PLATIN SPONSOREN



GOLD SPONSOREN



SILBER SPONSOREN



STARTUP SPONSOREN



MEDIEN SPONSOREN





www.m365-summit.de

Die Konferenz rund um Microsoft 365